AMENDMENTS TO THE CLAIMS

Amended claims follow:

1. (Currently Amended) A computer-implemented method for execution with computer code embodied on a tangible computer readable medium for detecting intrusions on a network, comprising:

storing signature profiles identifying patterns associated with network intrusions in a signature database;

generating classification rules based on said signature profiles;

receiving data packets transmitted on the network;

classifying data packets having corresponding classification rules according to said generated classification rules;

forwarding said classified packets to a signature engine for comparison with signature profiles; and

performing a table lookup to select an action to be performed on said classified packets based on the classification;

wherein the classification is carried out by a first classification stage capable of classifying the data packets based on a first set of packet characteristics, and a second classification stage capable of classifying the data packets received from the first classification stage based on a second set of packet characteristics;

wherein one of the actions is comparing said classified packets to at least a subset of the signature profiles;

wherein the first set of packet characteristics on which the classification of the first classification stage is based includes at least one of a destination address, a protocol type, and a destination port number;

wherein the second set of packet characteristics on which the classification of the second classification stage is based includes at least one of a packet type and a size;

wherein classifying said data packets comprises classifying said data packets according to at least one packet field into groups, and classifying said data packets within each of the groups according to TCP flags;

wherein the second classification stage remains in communication with a flow table for identifying an action to be taken with respect to the data packets;

wherein the action identified utilizing the flow table includes dropping at least one of the data packets and updating one or more fields in the flow table;

wherein the first classification stage precedes the second classification stage.

2. (Original) The method of claim 1 further comprising dropping data packets without corresponding classification rules.

3. – 5. (Cancelled)

6. (Currently Amended) The method of claim [[4]]1 ~~wherein classifying said packets according to packet size or type comprises~~ further comprising classifying said data packets within each of the groups according to packet length.

7. (Currently Amended) The method of claim [[3]]1 wherein classifying said data packets according to the at least one packet field comprises classifying said data packets according to protocol type.

8. (Currently Amended) The method of claim [[3]]1 wherein classifying said data packets according to the at least one packet field comprises classifying said data packets according to destination port number.

9. (Currently Amended) The method of claim [[3]]1 wherein classifying said data packets according to the at least one packet field comprises classifying said data packets according to destination address.

10. (Cancelled)

11. (Cancelled)

12. (Currently Amended) The method of claim 1 wherein one of the actions of the table is dropping [[the]]the at least one of the data packets.

13. (Previously Presented) The method of claim 1 further comprising generating an alert following the table lookup.

14. (Currently Amended) The method of claim 1 wherein the table lookup is performed in [[a]]the flow table and further comprising updating a field of the flow table.

15. (Original) The method of claim 1 further comprising partitioning signatures into disjoint groups to define subsets of signature profiles.

16. (Currently Amended) The method of claim 15 further comprising comparing said data packets to at least one of the subsets of signature profiles.

17. (Currently Amended) The method of claim 1 further comprising filtering said received data packets.

18. (Currently Amended) The method of claim 1 wherein receiving said data packets comprises capturing said data packets at a network analysis device.

19. (Original) The method of claim 18 further comprising decoding protocols after receiving said packets.

20. (Currently Amended) An intrusion detection system including a tangible computer readable medium comprising:

a signature classifier comprising a first stage classifier operable to classify packets according to at least one packet field into groups during a first classification stage, and a second stage classifier operable to classify said packets within each of the groups according to ~~packet type or size~~TCP flags during a second classification stage;

a flow table configured to support table lookups of actions associated with classified packets;

a signature database for storing signature profiles identifying patterns associated with network intrusions; and

a detection engine operable to perform a table lookup at the flow table to select an action to be performed on said classified packets based on the classification, wherein comparing said classified packets to at least a subset of the signature profiles is one of the actions;

wherein classifying said packets according to at least one packet field during the first classification stage comprises classifying said packets according to at least one of a destination address, a protocol type, and a destination port number;

wherein the second classification stage remains in communication with the flow table for identifying the action to be performed on said classified packets;

wherein the action includes dropping at least one of said classified packets and updating one or more fields in the flow table;

wherein the first classification stage precedes the second classification stage.

21. (Original) The system of claim 20 further comprising a data monitoring device having a capture engine operable to capture data passing through the network and configured to monitor network traffic, decode protocols, and analyze received data.

22. (Previously Presented) The system of claim 21 further comprising application program interfaces configured to allow the intrusion detection system access to applications of the data monitoring device to perform intrusion detection.

23. (Original) The system of claim 21 further comprising a parser operable to parse, generate, and load signatures at the detection engine.

24. (Original) The system of claim 21 further comprising an alarm manager operable to generate alarms.

25. (Original) The system of claim 21 further comprising a filter configured to filter out packets received at the intrusion detection system.

26. (Original) The system of claim 21 further comprising a capture engine configured to forward packets and temporarily store packets for later analysis by the data monitoring device.

27. (Original) The system of claim 20 wherein the flow table is a hash table.

28. (Currently Amended) The system of claim 20 wherein action options listed in the flow table include the dropping the at least one of said classified packets and generating an alarm.

29. (Currently Amended) The system of claim 28 wherein the action options further include the dropping the at least one of said classified packets and the updating the one or more fields of the flow table.

30. (Currently Amended) A computer program product embodied on a tangible computer readable medium for detecting intrusions on a network, comprising:

code that stores signature profiles identifying patterns associated with network intrusions in a signature database;

code that generates classification rules based on said signature profiles;

code that receives data packets transmitted on the network;

code that classifies data packets having corresponding classification rules according to said generated classification rules;

code that forwards said classified packets to a signature engine for comparison with signature profiles and stores signature profiles identifying patterns associated with network intrusions in a signature database; and

code that performs a table lookup to select an action to be performed on said classified packets based on the classification;

wherein the classification is carried out by a first classification stage capable of classifying the data packets based on a first set of packet characteristics, and a second classification stage capable of classifying the data packets received from the first classification stage based on a second set of packet characteristics;

wherein one of the actions is comparing said classified packets to at least a subset of the signature profiles;

wherein the first set of packet characteristics on which the classification of the first classification stage is based includes at least one of a destination address, a protocol type, and a destination port number;

wherein the second set of packet characteristics on which the classification of the second classification stage is based includes at least one of a packet type and a size;

wherein classifying said data packets comprises classifying said data packets according to at least one packet field into groups, and classifying said data packets within each of the groups according to TCP flags;

wherein the second classification stage remains in communication with a flow table for identifying an action to be taken with respect to the data packets;

wherein the action identified utilizing the flow table includes dropping at least one of the data packets and updating one or more fields in the flow table;

wherein the first classification stage precedes the second classification stage.

31. (Previously Presented) The method of claim 1, wherein the first set of packet characteristics includes the destination address, the protocol type, and the destination port number.

32. (Previously Presented) The method of claim 1, wherein the second set of packet characteristics includes the packet type and the size.

33. (Cancelled)

34. (Currently Amended) The method of claim [[33]]1, wherein the flow table is at least one hash table.

35. (Previously Presented) The method of claim 1, wherein the classification rules are generated after filtering the data packets.

36. (Cancelled)

37. (Previously Presented) The method of claim 32, wherein the packet type is determined based on a TCP flag.

38. (Cancelled)

39. (New) The method of claim 1, wherein the signature engine uses a priority scheme to ensure that a subset of the signature profiles are compared with the classified packets based on a number of the data packets received.

40. (New) The method of claim 1, wherein the action identified utilizing the flow table includes dropping all unclassified packets.